2006-09

FORCEnet Implications for a Coalition Maritime Force

Gregory A. Miller

11th ICCRTS

COALITION COMMAND AND CONTROL IN THE NETWORKED ERA

FORCEnet Implications for a Coalition Maritime Force

Gregory A. Miller
Systems Engineering Department
Naval Postgraduate School
Monterey, CA 93943
831-656-2957
gamiller@nps.edu

John M. Green
Systems Engineering Department
Naval Postgraduate School
Monterey, CA 93943
jmgreen@nps.edu

FORCEnet Implications for a Coalition Maritime Force

Gregory A. Miller
Systems Engineering Department
Naval Postgraduate School
Monterey, CA 93943
gamiller@nps.edu

John M. Green
Systems Engineering Department
Naval Postgraduate School
Monterey, CA 93943
jmgreen@nps.edu

Abstract

U.S. members of the Technical Cooperative Program (TTCP) and the Naval Postgraduate School continue the work of an earlier Action Group on coalition network centric maritime warfare. The current terms of reference require defining in functional terms the levels of coalition interoperability with FORCEnet and assessing the incremental value of higher levels of interoperability as input to national balance of investment studies. The goal was to develop a high-level system architecture for C4ISR in a coalition maritime force. Four student teams followed U.S. DoD instructions for applying systems engineering in a capabilities-based approach, examining all DOTMLPF implications. The result was four Capabilities Development Documents with supporting DoD Architecture Framework products.

To provide a common basis to compare different architectures, three tactical situations were used. This bounded the scope of the problem by listing the blue force and red force platforms. Focusing on a specific non-combat operation, a littoral defense operation, and a littoral strike operation provided the foundation for measures of effectiveness in the comparison.

Modeling and simulation of the architectures with a PC-based discrete event simulation tool was completed. The results indicate a clear advantage to coalition platforms operating in a true network-centric fashion, with quantifiable improvements in red force attrition, blue force protection and weapons efficiency.

Introduction

FORCEnet is the US Navy's instantiation of network centric warfare.[1] It encompasses both the materiel and non-materiel solutions required to harness information networking to achieve an order of magnitude increase in combat power, increased efficiency and flexibility in force structure, and improved ability to overcome new asymmetric threats. FORCEnet development for coalition operational environments is nascent. Successful materiel solutions dedicated to providing human-centered command and control support have been fielded outside of traditional acquisition processes (early versions of coalition wide-area networks (COWAN) fielded in the Pacific area of operations). Indeed, realizing a complete information-age transformation of the maritime forces of just a single nation is a long-term and challenging goal.

Given the enormous investment of resources implied in realizing these war-fighting advantages, the questions for any long-term US ally are: Should we make the same investment in order to maintain interoperability? How can we quantify the costs and benefits resulting from such a decision? In the course of their usual business, The Technical Cooperation Program (TTCP)* Maritime Systems Group (MAR) has taken on the task of helping answer those questions.

Background

In early 2004, TTCP chartered an Action Group (AG-1) on coalition network-centric maritime warfare analysis to address a perceived lack of quantitative analysis in this area, and assist in program development.[2] AG-1 established two projects to study NCMW in breadth and depth, and completed its work in September 2004.

Action Group (AG-6) was chartered to extend the work to examine the implications of FORCEnet for a coalition maritime force. AG-6 is expected to offer significant mutual benefit by providing timely insights and guidance that will enable harmonizing national coalition C4I interoperability strategies and development plans. Their terms of reference are:

- Build on results and findings of AG-1 and initiate a follow-on study – FORCEnet Implications for Coalitions
- Examine the implications and way ahead for realizing coalition capabilities that are compatible with both the functionality and the timeline of the U.S. Navy's FORCEnet initiative
- MAR leadership seeks to define in functional terms the various levels of coalition interoperability with FORCEnet and to assess the incremental value of higher levels of interoperability to provide input to national balance of investment studies
- A transnational need is also recognized to harmonize national NCMW functional and technical roadmaps to support effective netted coalition capabilities and assessment of priorities

More specifically, "MAR directs AG-6 to pick one or two challenging scenarios in the littoral that capitalize on Fn and examine its benefits and undertake a sensitivity analysis."[3]

Members of TTCP agreed with Naval Postgraduate School faculty members that the above problem was a worthy topic for student research. Indeed, the timing was such that two separate cohorts of students enrolled in the Masters of Science in Systems

* TTCP is a collaborative exchange program in non-nuclear defense science and technology between the governments of Australia, Canada, New Zealand, United Kingdom and United States.

Engineering program were just starting their capstone project. The capstone project serves as a final synthesis of the entire SE curriculum. It brings together as many elements of the curriculum as possible in a comprehensive overview of the components and underlying technologies of modern warfare. In short, it is an opportunity for our students to prove they can “do” systems engineering: decompose complex problems, propose rational solutions, analyze and recommend the best solution, and communicate the results. Of course, this is all done with the tools and processes required of any DoD system proposal from a complete doctrine, organization, training, materiel, logistics, personnel & leadership, and facilities (DOTMLPF) perspective.[4]

The project’s overall purpose was to provide analysis and guidance on the tactical and technical requirements for coalition maritime warfare interoperability. Emphasis was placed on the alignment of coalition national acquisition strategies with FORCEnet. The goal was to develop a high-level system architecture to accomplish the specified missions in a true network-centric fashion. The final report was in the form of a Capabilities Development Document with supporting products from the DoD Architecture Framework as outlined in Chairman of the Joint Chiefs of Staff Instruction 3170.01C, Joint Capabilities Integration and Development System.

Approach and Task Scope

The approach was to define in functional terms various levels of interoperability with FORCEnet, to assess the incremental value of higher levels of interoperability via coalition strike group modeling and simulation, and to provide input to national balance of investment studies. Emphasis was placed on military operations in the littorals. Additionally, to limit the scope of the project and to provide a framework for realistic measures of effectiveness, three tactical situations were provided. All were to take place in the 2010-2015 time frame, consistent with the goals of AG-6, so the results could be used to affect FY08 investment decisions. The scenarios agreed upon by the key stakeholders were:

- A non-combatant evacuation of an island nation in the face of coup sponsored by a near-peer competitor.
- Repel a threatening invasion force by a near-peer competitor of a smaller, less well-defended ally.
- Re-establish sovereignty on a disputed island that was wrongfully occupied by a near-peer competitor.

The major platforms participating in a coalition force were also defined. They were composed of mostly US ships with ships from other nations participating. There would be a carrier strike group and an expeditionary strike group.

Because of the size of the class, the students were divided into 4 teams:

1. Carrier strike group, with emphasis on surface and anti-air warfare
2. Expeditionary strike group, with emphasis on surface and anti-air warfare
3. Carrier strike group, with emphasis on submarine and mine warfare
4. Expeditionary strike group, with emphasis on submarine and mine warfare

Given that the students were civilian employees of Naval Surface Warfare Center in Port Hueneme, CA and Naval Undersea Warfare Center in Keyport, WA, this separation based on warfare domains seemed logical.

The student teams started with a gap analysis between "as-is" architectures and the required capabilities of a truly network-enabled force. The "as-is" architectures were based on those systems in use during the RIMPAC 04 exercise and Trident Warrior 04 experiments.[5] They developed C4ISR system architectures that provided the functional capabilities required of network-centric forces. A complete DOTMLPF spectrum was examined, including changes to doctrine on security enclaves and strike group organization to achieve force-level data fusion of all engagement quality track information.

The architectures were modeled using a commercially available discrete-event simulation tool (Extend by ImagineThat, Inc.) Several of the more technically challenging aspects of creating and sharing common operational pictures, such as data fusion, and sharing engagement-quality track data were modeled in a very rudimentary way. Threat analysis and weapons assignment algorithms were kept simple. Other simplifying assumptions common to all groups was the availability of bandwidth; system reliability; and information assurance. While in reality, we know that data throughput between battlespace entities is limited by their access to shared assets like satellite communication systems; we wanted to focus on how those connections were used. No system failures were modeled for this first exercise. Offensive information operations by red and blue forces were also not modeled in this project. The point was to examine the functional capabilities of network centricity and analyze the effectiveness of a force operating under net-centric concepts compared to one operating with as-is concepts. Simulations were run with "full" FORCEnet, "partial" FORCEnet, and no FORCEnet. The platforms with their organic sensor and weapon systems (with the associated probabilities of detection and probabilities of kill) were kept the same between simulations. Only the connectivity and allowable emergent behavior were varied.

All groups created similar system architectures. This is to be expected, given the common problem and common required capabilities of each group. Figure 1 shows the OV-1 High-Level Operational Concept Graphic from the AAW- and ASuW-focused CSG team.[6] It is worthy to note that non-US assets are depicted as equal partners in the strike group. All the key enablers for network centricity are identified as attributes of the network and the use of out-of-theater ISR assets is considered. Figure 2 and Figure 3 show the OV-5 Operational Activity Model from the AAW- and ASuW-focused ESG team.[7] All teams were directed to start with the warfighters' mission in mind. So, it is not surprising again that each team created products that were similar and patterned after the classic observe-orient-decide-act paradigm. The DoD Architecture Framework does not specify a single modeling language for any of the required graphical products. As our students have all been exposed to IDEF0, Hatley-Pirbhai, UML, and several other tools, we found a mix of all of them in the final products delivered.

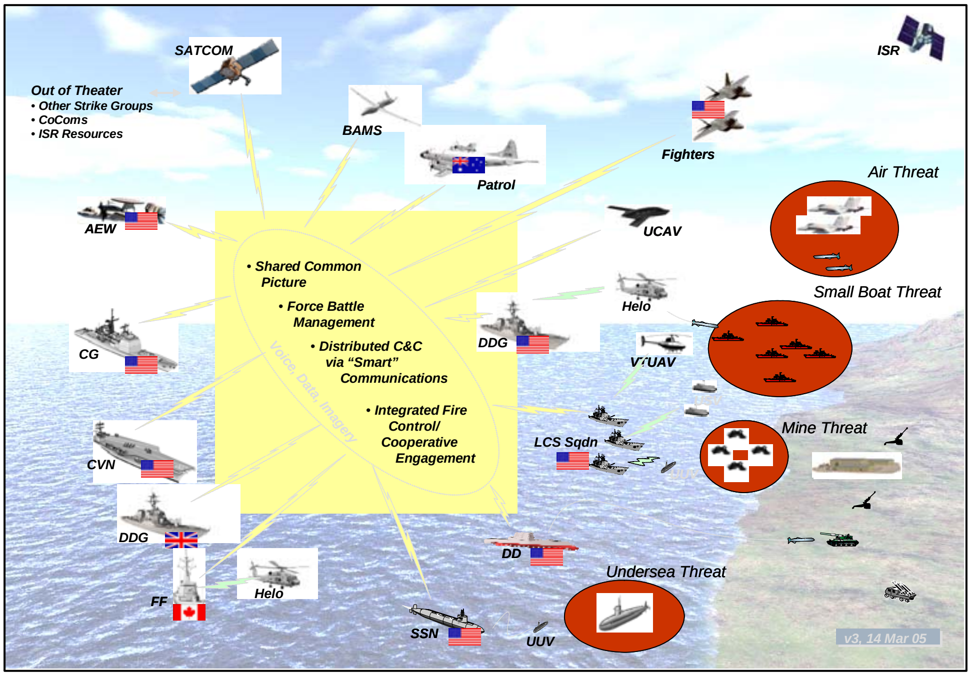

Figure 1: OV-1 High-Level Operational Concept Graphic

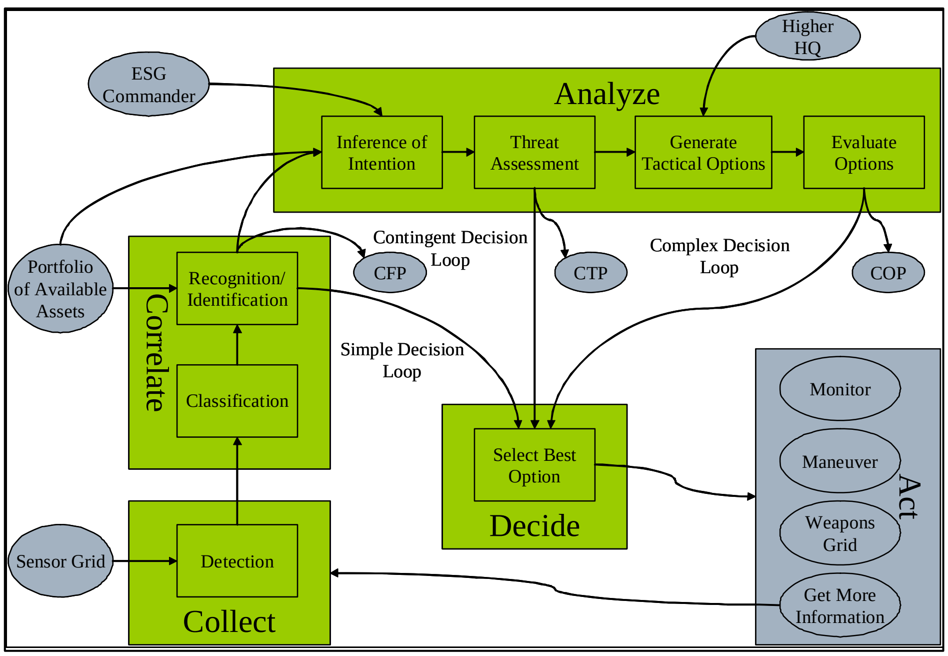

Figure 2: OV-5 Operational Activity Model (Top Level)

The modeling and simulation conducted were based on the lower levels of abstraction of this OV-5 Operational Activity Model. Figure 4 shows the high level block diagram of the model used and Figure 5 provides some detail in the interaction between the spreadsheet used for detection and engagement calculation and the discrete-event simulation. Figure 6 shows the final Extend model used.

Students created all hierarchical blocks and linked sensor and weapon performance based on effectiveness estimates found in the open literature. Each group approached the modeling problem in a similar manner.

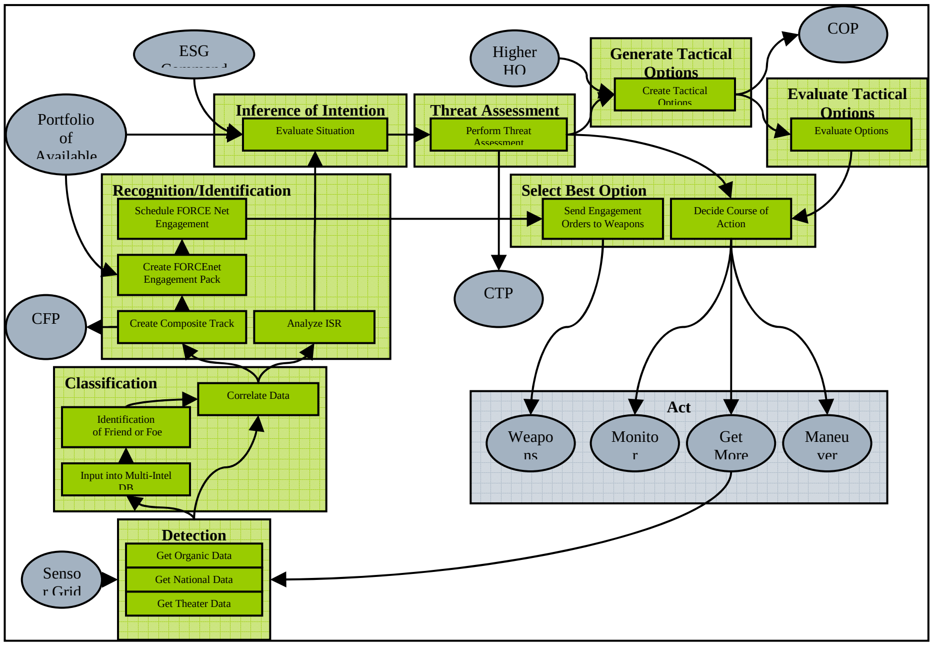

Figure 3: OV-5 Operational Activity Model (Level 1)

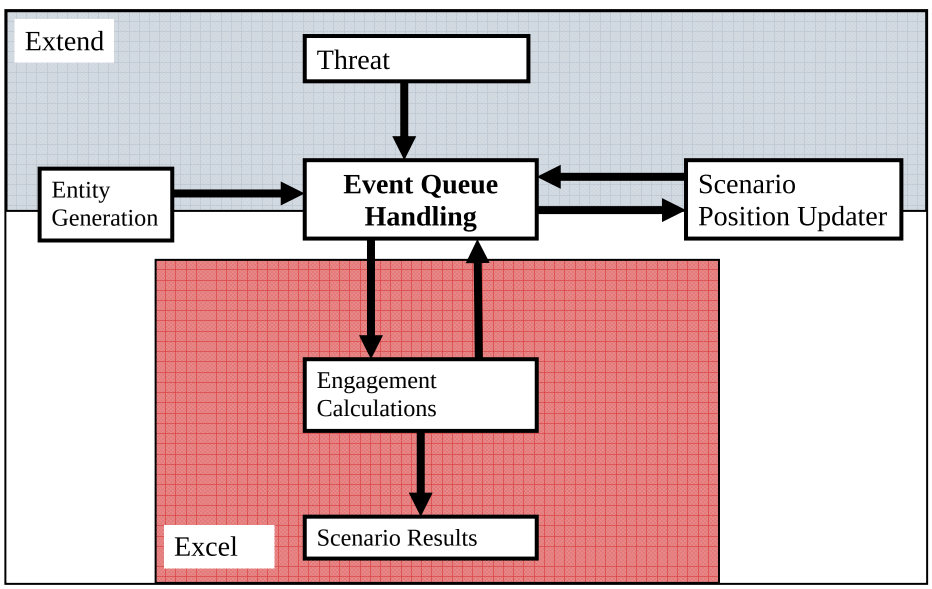

Figure 4: Model Block Diagram

The differences were, for the most part, minor. The red forces and blue forces are represented as items passing through the blocks. Each has its own sensors and weapons and they are tracked based on their geographic location. Their interaction is simulated in each block. This included platform movement, detections, and engagements. Each time step of the simulation allowed the platforms to move, new detections and updates to existing tracks were made, and weapon engagements (if any) were processes based on estimated effectiveness probabilities compared to random numbers generators.

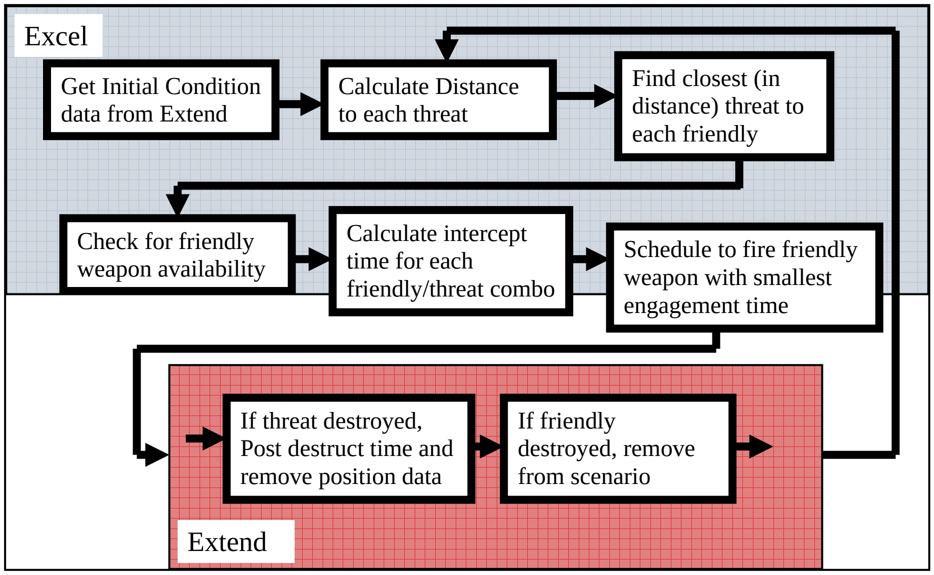

Figure 5: Model Detail

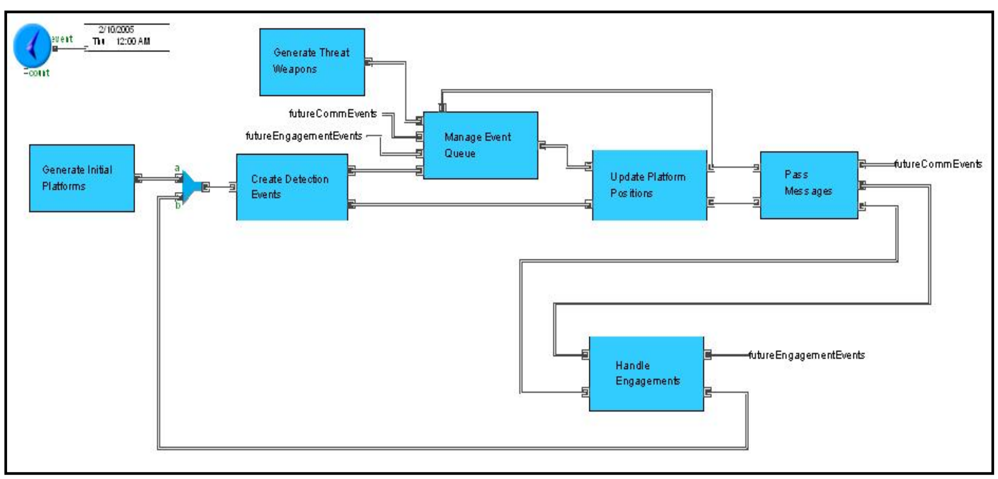

Figure 6: Extend Model

In the "with FORCEnet" scenarios, the "pass messages" block updated the blue force's common operational picture with fused data and ensured that all platforms had the data. The most powerful aspect of the students' architecture design is evidenced in this block as no distinction is made between platforms based on nationality. The "handle engagements" block performed group-wide threat evaluation and weapons assignment and went on to assess the effectiveness of each engagement. Red on blue engagements were executed in this block as well. In the "no FORCEnet" scenario, the "pass messages" block did not permit cross-platform data fusion or information sharing. The "handle engagements" block only computed engagements based on each platform's organic sensor information.

The simulations were conducted to quantify the effectiveness of FORCEnet operations. That is, metrics were gathered over many iterations of the model and translated into operational measures of effectiveness (MOEs). Measures of effectiveness were chosen by students based on our guidance. Emphasis was on war-fighter effectiveness, consistent with JCIDS direction and good systems engineering practice. That is, attributes specific to sub-systems such as latency, packet loss, etc, were not analyzed in detail. Rather, measures that specifically have meaning for the war-fighter were analyzed. For example, number and percentage of red forces countered over a fixed time, number and percentage of blue forces surviving over a fixed time, and overall force-level weapon efficiency. A typical set of MOEs with supporting measures of performance (MOP) is listed in the below table.[8]

MOE 1	Capability to evaluate pre-engagement situation: In this, the Observation Phase of an operation, the battle force must determine the presence, capability, and projected intent of hostile forces.	
	MOP a)	Measure ability to maintain track on all active tracks
	MOP b)	Measure percent of operating area (OPAREA) occupied by opposing forces
	MOP c)	Objective measure degree of confidence in intelligence data
	MOP d)	Measure separation between hostiles and allies/non-combatants
	MOP e)	Measure hostile movement
	MOP f)	Categorize enemy presence
MOE 2	Determine scope of battle-space: Measure anticipated impact of weather predictions on communications, ability to prioritize threats.	
MOE 3	Capability to determine posture and orientation of the mission.	
	MOP a)	Measure of evacuees to extract per capabilities
	MOP b)	Readiness of equipment per system
	MOP c)	Ratio of weapons per threat
	MOP d)	Measure sortie rate available
	MOP e)	Objective measure of anticipated impact of weather predictions on operations and communications
MOE 4	Ability to translate commanders' decisions into plans and orders.	
	MOP a)	Ability to maintain track on all active tracks
	MOP b)	Battle field picture refresh rate
	MOP c)	Objective measure of information completeness
	MOP d)	Maximum number of different military units that can be connected to command when needed
	MOP e)	Number of requests for clarification regarding previously distributed commander's intent
	MOP f)	Number of mishaps due to friendly fire
MOE 5	Capability to carry out prescribed response during mission.	
	MOP a)	Probability of kill
	MOP b)	Casualty rates
	MOP c)	Effectiveness of system for MOOTH
	MOP d)	Number of operations redirected before completion as result of enemy reactions
MOE 6	System Suitability: Improved connectivity between systems comes at a cost to operational units. The connectivity must be established, maintained, and periodically changed to comply with changing situations. The time required to accomplish these tasks are in addition to any existing C4I system requirements, but should significantly reduce the operational load on those other systems.	
	MOP a)	Amount of time required to establish communications network
	MOP b)	Amount of time required to perform maintenance
	MOP c)	Percentage of time communication network operational
	MOP d)	Number of units reporting loss of connection
	MOP e)	Number of operational tasks not accomplished or negatively impacted by loss of communications

Results

The four student teams delivered reports that, understandably, exhibited many similarities and a few differences with each other. This paper seeks to present those aspects of the reports that speak directly to comparing the proposed "purely" network-centric architectures with those in use today. One group did report an unusual result that will be discussed shortly.

Due to time constraints, not all MOEs were measured, but only those that focused on the self-defense aspects of the scenarios rather than on the offensive aspects. For example, from the above list, only the following were measured:

- Number and percentage of red platforms tracked
- Number of engagements
- Number and percentage of red force hard kills
- Number and percentage of blue force attrition
- Time to send engagement and platform status

In general, the total combat effectiveness of the coalition force was improved in terms of number of red force attrition, blue force survival, engagement sustainability, and hard-kill weapons efficiency. With FORCEnet, statistics for red detections in the operational area show an increase of 70 to 100% at any time step. This enabled faster engagements. The statistics show that roughly 50% of all kills and 50% of all engagements happen quicker with FORCEnet. Other groups couched this speed of engagement result as a reduction in time from initial detection to engagement. Improvements of 22 to 41% were noted. Efficiency in terms of number of weapons used improved by 20 to 50%. Another benefit shown by the model is a 45% reduction of blue force cumulative attrition. Surprisingly, the number of red forces killed increased by only 10 to 15%. Also, the measure of raid annihilation proved inconclusive with improvements of only a few percent.

One of the more striking results was the increase in potential number of weapons on a target as an indicator of effective engagement envelope improvement. That is, for purposes of weapon assignment, the netted force had more options with regard to which platform could engage an enemy. Figure 7 (taken from one simulation) shows this quite clearly.[9]

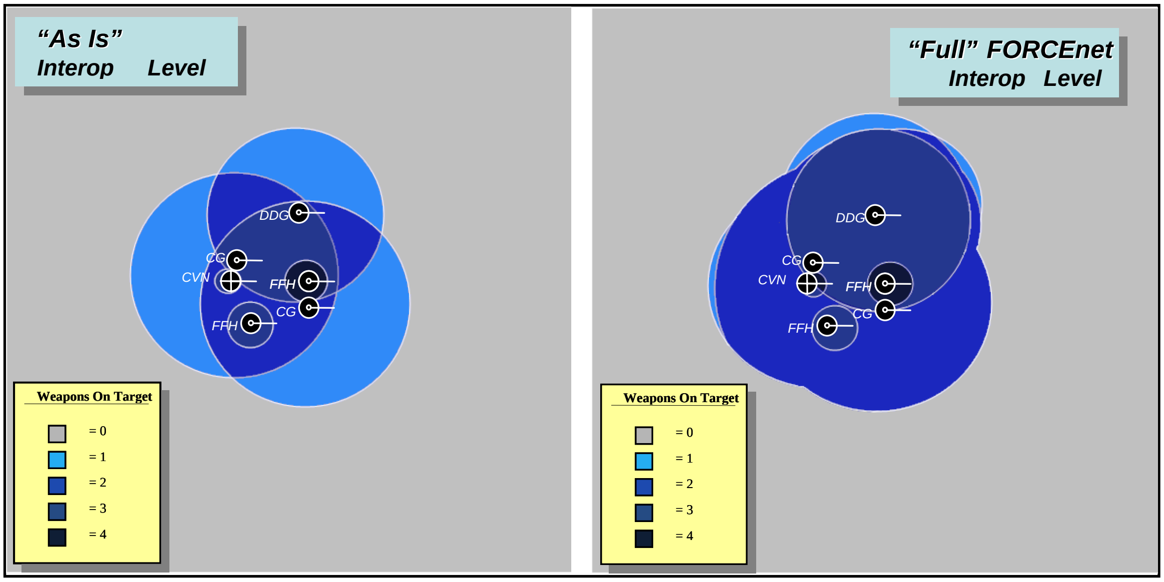

Figure 7: Increase in weapons on target

The shades of blue vary with the number of weapons that could engage a target in each respective area. The figure on the left shows that each platform can only engage those targets tracked with organic sensors. In network-centric simulations, they can engage targets tracked by any platform's sensors. The figure on the right shows that this translates into more potential weapons on target. What that means to the warfighter is increased efficiency in automatically selecting the optimum weapon across the entire group and more engagement opportunities resulting in an increased probability of kill. Both of these results are supported by the metrics gathered in the simulations.

However, these advantages come with a price. All simulations showed an increase in data throughput between all blue force platforms by as much as 150%. Additionally, one group did manage an "almost FORCEnet" scenario in which only the US forces worked in a network centric fashion while the other platforms participated in a traditional way.[10] None of the advantages of network centricity were realized, indicating it's an "all or nothing" proposition.

The unusual result referred to in the beginning of this section occurred because one group placed less capable (non-FORCEnet) platforms in the outer screens of the battlegroup. The net result was a reduction in overall performance of the battlegroup because of an increase in overall system response times. Analysis of the scenario quickly pinpointed the cause of the anomaly and the scenario was re-run with results consistent with the rest of the analysis. It did highlight the fact that care must be taken in how ships are positioned when there is a mixture of capable and less capable ships.

The study was considered a success. It quantified the effectiveness of coalition FORCEnet in terms that are directly applicable to war fighting capability. Even though some results were inconclusive, the members of TTCP's AG-6 from five different nations appreciate the advantage of having a partial answer to the question "how much is a pound of FORCEnet worth." They have incorporated the results and lessons learned into their overall study plan.

Ongoing and Future Work

The group of students currently involved in the follow-on analytic work has fewer students than the original groups. However, like before, they come from two different classes and they are divided between two localities. They will revisit the ESG portion of the study using a Philippine humanitarian relief scenario with eight vignettes that add some granularity to the communications architecture based on planned coalition "C2 Order of Battle." Each group is working independently, but their goals are the same. Specifically, their goal is to conduct a sensitivity analysis to determine if there is a "knee in the curve" of effectiveness versus investment cost, and to analyze enemy use of more pervasive information warfare on the coalition C2 architecture.

The nature of the ESG lends itself to accommodating coalition enhancements to give a scalable and composable force. The intent of the study is to quantify the degree to which FORCEnet (Fn) improves the probability of successfully completing its mission. Specific ESG coalition capability options to explore in the modeling are shown in the below table.

Option	Description
I (do nothing)	Small size (all US) ESG force, fully Fn capable
II (do minimum)	Added Coalition ships, but not Fn capable (i.e. larger overall force)
III	Intermediate Fn capability to the additional Coalition ships
IV	Full Fn capability to entire force

One major difference between the results presented in this paper and the current work is that the Concept of Analysis (CoA) for AG-6 modeling now includes both high- and low-level operational Analysis (OA). The high level work is essentially at the campaign outcome level, while the lower level work is at the vignette or encounter level. This work is recognized as an integral part of the AG-6 overall study plan and will be incorporated into that group's final report.

Notes

[1] Space and Naval Warfare Systems Command. *A Concept for FORCEnet*. San Diego, CA, November 2004.
[2] The Technical Cooperation Program. *Key Issues in Coalition Network-Centric Maritime Warfare*. TTCP Technical Report TR-MAR-10-2003. January, 2004.
[3] The Technical Cooperation Program AG-6 Terms of Reference, October 2003.
[4] Naval Postgraduate School Department of Systems Engineering web site accessed 21 March 2006. http://www.nps.navy.mil/se/
[5] Boe, Heath, et al. *FORCEnet Implications for a Coalition Maritime Force, Focus on ESG.* Master of Science in Systems Engineering Integrated Project Report, Naval Postgraduate School, NUWC Keyport Cohort, June 2005.
[6] Bailey, Robert, et al. *FORCEnet Implications for a Coalition Maritime Force, Focus on CSG.* Master of Science in Systems Engineering Integrated Project Report, Naval Postgraduate School, NSWC Port Hueneme Cohort, June 2005.
[7] Carnes, Joseph, et al. *FORCEnet Implications for a Coalition Maritime Force, Focus on ESG.* Master of Science in Systems Engineering Integrated Project Report, Naval Postgraduate School, NSWC Port Hueneme Cohort, June 2005.
[8] Bennett, Lara, et al. *FORCEnet Implications for a Coalition Maritime Force, Focus on CSG.* Master of Science in Systems Engineering Integrated Project Report, Naval Postgraduate School, NUWC Keyport Cohort, June 2005.
[9] Bailey, et al.
[10] Bailey, et al.